EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ido Rabinovitch (Reg. No. L0080) on 11/2/10.

The application has been amended as follows:

Listing of Claims

The following listing of claims replaces prior listings.

1. (Currently Amended) An apparatus, comprising:

a determiner, comprising one or more programmable hardware-based processing elements, configured to determine whether a message, comprising a session initiation protocol message, received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer, the message comprising a second layer identity header;

a forwarder, comprising the one or more programmable hardware-based processing elements, configured to forward the message within the first network regardless of the result of the determination; and

a modifier, comprising the one or more programmable hardware-based processing elements, configured to modify the message so as to remove at least part of the second layer identity header ~~include a second layer indication~~ to indicate that the message has not been through the security check applied at a ~~security~~ secure Za interface between two security domains prior to being received at the first network when the result of the determination is that the message has not been through the security check, wherein the second layer is a higher layer than the first layer;

wherein the forwarder is further configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the ~~security~~ Za interface prior to being received at the first network.

2. (Previously Presented) The apparatus according to claim 1, further comprising:

a receiver configured to receive messages via a secure interface and a second network and directly from outside the first network.

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Currently Amended) The apparatus according to claim [[4]] 1, wherein the identity header comprises a p-asserted identity.

7. (Cancelled)

8. (Currently Amended) The apparatus according to claim [[7]] 1, further comprising:

a detector configured to detect whether the second layer identity header is of a particular type and when so to remove at least part of the header.

9. (Cancelled)

10. (Previously Presented) The apparatus according to claim 8, wherein the detector is configured to detect whether the second layer identity header comprises a p-asserted identity.

11. (Cancelled)

12. (Cancelled)

13. (Previously Presented) The apparatus according to claim 1, wherein the apparatus comprises an interrogating call session control function.

14.-21. (Cancelled)

22. (Currently Amended) A system, comprising:

a security server comprising one or more programmable hardware-based processing elements; and

a network processing element, comprising the one or more programmable hardware-based processing elements, the security server being configured to receive a message comprising a session initiation protocol message, the session initiation protocol message including a second layer identity header, the security server further configured to determine whether the message has been through a security check by determining whether or not the message has been received with security at a first layer, when the result of the determination is that the message has not been through the security check applied at a ~~security~~ secure Za interface between two security domains modify the message so as to remove at least part of the second layer identity header include ~~a second layer indication~~ to indicate that the message has not been through the security check applied at the ~~security~~ Za interface prior to being received at the security server, wherein the second layer is a higher layer than the first layer, and forward the message regardless of the result of the determination;

wherein the network processing element is configured to forward the message without modification in response to the determination being that the message has been through the security check applied at the ~~security~~ Za interface prior to being received at the first network.

23. (Cancelled)

24. (Cancelled)

25. (Currently Amended) A method, comprising:

determining, at one or more programmable hardware-based processing elements, that a message comprising a session initiation protocol message received at a first network has not been through a security check by determining that the message has not been received with security at a first layer, the message comprising a second layer identity header;

modifying, at the one or more programmable hardware-based processing elements, the message so as to remove at least part of the second layer identity header ~~include a second layer indication~~ to indicate that the message has not been through the security check applied at a ~~security~~ secure Za interface between two security domains prior to being received at the first network, wherein the second layer is a higher layer than the first layer; and

forwarding, at one or more programmable hardware-based processing elements, the message within the first network;

wherein forwarding the message includes forwarding the message without modification in response to the determination being that the message has been through the security check applied at the ~~security~~ Za interface prior to being received at the first network.

26.-45. (Cancelled)

46. (Currently Amended) An apparatus, comprising:

determining means, comprising one or more programmable hardware-based processing elements, for determining whether a message comprising a session initiation protocol message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer, the message comprising a second layer identity header;

modifying means, comprising the one or more programmable hardware-based processing elements, for, when the message is determined not to have been through the security check, modifying the message to remove at least part of the second layer identity header ~~include a second layer indication~~ to indicate that the message has not been through the security check applied at a ~~security~~ secure Za interface between two security domains prior to being received at the first network, wherein the second layer is a higher layer than the first layer; and

forwarding means, comprising the one or more programmable hardware-based processing elements, for forwarding the message within the telecommunications network regardless of whether the message has been through a security check;

wherein the forwarding means is further configured for forwarding the message without modification in response to the determination being that the message has been through the security check applied at the ~~security~~ Za interface prior to being received at the first network.

47.-55. (Cancelled)

56. (Cancelled)

57. (Cancelled)

58. (Currently Amended) The method according to claim [[56]] 25, wherein the identity header comprises a p-asserted identity.

59. (Cancelled)

60. (Previously Presented) The method according to claim 25, further comprising:

detecting whether the second layer identity header is of a particular type and when so removing at least part of the header.

61. (Cancelled)

62. (Currently Amended) The method according to claim [[61]] 60, further comprising:

detecting whether the second layer identity header comprises a p-asserted identity type.

63. (Cancelled)

64. (Cancelled)

65. (Previously Presented) The apparatus according to claim 1, wherein the forwarder is configured to forward the message over a Zb interface.

66. (Cancelled)

67. (Cancelled)

68. (Previously Presented) The system according to claim 22, wherein the security server is configured to forward the message to the network processing element over a Zb interface.

69. (Cancelled).

70. (Cancelled)

71. (Previously Presented) The method according to claim 25, comprising forwarding the message within the first network over a Zb interface.

2. The following is an examiner's statement of reasons for allowance: Currently presented claims 1, 22, 25 and 46 recite a message processing processes, claimed explicitly for processing Session Initiation Protocol (SIP) messages. Said claims further specify that when a message is not received via "Za" interface, at least part of an identity header is removed.

The closest prior art includes, Jennings (RFC 3325 Internet Draft, http://tools.ietf.org/html/draft-ietf-sip-asserted-identity-00, May 27, 2002), Marshall (draft-ietf-sip-privacy-04.txt, February 27, 2002) and 3GPP (3GPP TSG SA WG3 Security – S3#18, Proposed changes to 33.2000 about Za, Zb, Zc interfaces), applied in the final rejection as Jennings in view of Marshall and Peterson. Jennings in view of Marshall and Peterson, like Applicant's claim language, is directed to processing SIP messages (Marshall, pg. 2, see "Scope of Applicability"), and includes teachings regarding identity headers and Za interfaces (3GPP, Fig. 1). However, the prior art does not teach the entirety of the pending independent claims; specifically the prior art does not teach or suggest all of, when considered as a whole as presented in the pending independent claims, processing messages comprising SIP messages, removing part of a second layer identity header, to indicate a message has not be though a security check applied at the claimed Za interface in the claimed forwarding environment. This conclusion based on Applicant's discussion of the Za interface, which is a specific type of interface with a particular implementation in the SIP environment of Applicant's

claims. For example, Applicants Specification states on pages 6 – 7, paragraph 29, that:

> *The Za-interface covers all NDS/IP (Network Domain Security/Internet Protocol) traffic between security domains. The SEGs (Security Gateways) use IKE (Internet Key Exchange) to negotiate, establish and maintain a secure ESP (Encapsulating Security Payload) tunnel between them. Subject to roaming agreements, the inter-SEG tunnels would normally be available at all times, but they can also be established as needed. ESP shall be used with both encryption and authentication integrity, but an authentication/integrity only mode is allowed. The tunnel is subsequently used for forwarding NDS/IP traffic between security domain A and security domain B.*

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOHN M. MACILWINEN whose telephone number is (571)272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glen Burgess can be reached on (571) 272-3949. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JOHN MACILWINEN

571-272-9696

/KEVIN BATES/
Primary Examiner, Art Unit 2456